

THE HONORABLE _____

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

DOMAIN NAME COMMISSION
LIMITED,

Plaintiff,

v.

DOMAINTOOLS, LLC

Defendant.

No. 2:18-cv-874

DOMAIN NAME COMMISSION
LIMITED'S MOTION FOR PRELIMINARY
INJUNCTION

NOTE ON MOTION CALENDAR:
Friday, July 13, 2018

ORAL ARGUMENT REQUESTED

DNCL'S MOTION FOR PRELIMINARY
INJUNCTION (NO. 2:18-CV-874)

139655561.8

Perkins Coie LLP
1201 Third Avenue, Suite 4800
Seattle, WA 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	STATEMENT OF FACTS	2
	A. Domain Name Background and Terminology	2
	B. DNCL and the .nz WHOIS terms of use.....	4
	C. DomainTools and the present dispute.....	6
III.	ARGUMENT.....	7
	A. DNCL is entitled to a preliminary injunction enjoining DomainTools’s unlawful activities.	7
	1. DNCL is likely to succeed on the merits of its claims.....	7
	a. DNCL is likely to succeed on its claim that DomainTools breached DNCL’s terms of use.....	8
	b. DNCL is likely to succeed on its claim that DomainTools violated the Computer Fraud and Abuse Act.....	12
	c. DNCL is likely to succeed on its claim that DomainTools violated the Washington Unfair Competition Law.....	13
	2. DNCL is currently suffering and will continue to suffer irreparable harm without a preliminary injunction.	16
	a. DomainTools is causing irreparable harm to DNCL’s reputation and goodwill by depriving IRPO registrants of the privacy protection DNCL promised them.....	16
	b. DomainTools is causing DNCL to suffer irreparable harm to its reputation and goodwill because .nz registrants are not receiving the general protections promised in the TOU.	18
	c. DomainTools is causing DNCL irreparable harm because it will be forced to divert internal resources away from its organizational mission to police and prevent DomainTools’s unauthorized activity.....	20
	3. The balance of equities tips sharply towards DNCL.	21
	4. A preliminary injunction is in the public interest.	22
	B. No bond should be required.....	24
IV.	CONCLUSION.....	25

TABLE OF AUTHORITIES

CASES

<i>adidas Am., Inc. v. Skechers USA, Inc.</i> , 890 F.3d 747 (9th Cir. 2018)	17
<i>All. for the Wild Rockies v. Cottrell</i> , 632 F.3d 1127 (9th Cir. 2011)	22
<i>All. For the Wild Rockies v. Pena</i> , 865 F.3d 1211 (9th Cir. 2017)	6, 8, 22
<i>Berkson v. Gogo LLC</i> , 97 F. Supp. 3d 359 (E.D.N.Y. 2015)	9
<i>Boardman v. Pac. Seafood Grp.</i> , 822 F.3d 1011 (9th Cir. 2016)	23
<i>Cal. ex rel. Van De Kamp v. Tahoe Reg'l Planning Agency</i> , 766 F.2d 1319 (9th Cir. 1985)	25
<i>Caribbean Marine Servs. Co. v. Baldrige</i> , 844 F.2d 668 (9th Cir. 1988)	16
<i>Craigslist Inc. v. 3Taps Inc.</i> , 942 F. Supp. 2d 962 (N.D. Cal. 2013)	13
<i>Disney Enters., Inc. v. VidAngel, Inc.</i> , 869 F.3d 848 (9th Cir. 2017)	17
<i>Ehling v. Monmouth-Ocean Hosp. Serv. Corp.</i> , 961 F. Supp. 2d 659 (D.N.J. 2013)	15
<i>Facebook, Inc. v. Power Ventures, Inc.</i> , 844 F.3d 1058 (9th Cir. 2016), <i>cert denied</i> , 138 S. Ct. 313 (2017)	13
<i>Facebook, Inc. v. Power Ventures, Inc.</i> , No. C 08-5780 JF (RS), 2009 WL 1299698 (N.D. Cal. May 11, 2009)	9
<i>Fed. Trade Comm'n v. Sperry & Hutchinson Co.</i> , 405 U.S. 233 (1972)	14
<i>Garcia v. Google, Inc.</i> , 786 F.3d 733 (9th Cir. 2015) (en banc)	8

TABLE OF AUTHORITIES
(continued)

<i>Herb Reed Enters., LLC v. Fla. Entm't Mgmt., Inc.</i> , 736 F.3d 1239 (9th Cir. 2013)	17
<i>hiQ Labs, Inc. v. LinkedIn Corp.</i> , 273 F. Supp. 3d 1099 (N.D. Cal. 2017), <i>appeal docketed</i> , No. 17-16783 (9th Cir. Sept. 6, 2017)	13
<i>Klem v. Wash. Mut. Bank</i> , 176 Wn.2d 771 (2013)	14
<i>L.A. Mem'l Coliseum Comm'n v. Nat'l Football League</i> , 634 F.2d 1197 (9th Cir. 1980)	21
<i>Magney v. Lincoln Mut. Sav. Bank</i> , 34 Wn. App. 45 (1983)	14
<i>McKee v. Audible, Inc.</i> , No. CV 17-1941-GW(Ex), 2017 WL 4685039 (C.D. Cal. July 17, 2017)	9
<i>Michael v. Mosquera-Lacy</i> , 165 Wn.2d 595 (2009)	15
<i>Nguyen v. Barnes & Noble Inc.</i> , 763 F.3d 1171 (9th Cir. 2014)	8, 9
<i>Nordstrom, Inc. v. Tampourlos</i> , 107 Wn.2d 735 (1987)	15, 16
<i>Nw. Indep. Forest Mfrs. v. Dep't of Labor & Indus.</i> , 78 Wn. App. 707 (1995)	8
<i>Perfect 10, Inc. v. Google, Inc.</i> , 653 F.3d 976 (9th Cir. 2011)	22
<i>Rajagopalan v. NoteWorld, LLC</i> , No. C11-05574BHS, 2012 WL 727075 (W.D. Wash. Mar. 6, 2012), <i>aff'd</i> , 718 F.3d 844 (9th Cir. 2013)	15
<i>Ramos v. Arnold</i> , 141 Wn. App. 11, 20 (2007)	15
<i>Regents of University of Cal. v. Am. Broad. Cos., Inc.</i> , 747 F.2d 511 (9th Cir. 1984)	20

TABLE OF AUTHORITIES
(continued)

<i>Register.com, Inc. v. Verio, Inc.</i> , 356 F.3d 393 (2d Cir. 2004).....	9, 19, 20
<i>Rent-A-Ctr., Inc. v. Canyon Television & Appliance Rental, Inc.</i> , 944 F.2d 597 (9th Cir. 1991)	16
<i>Schnall v. AT&T Wireless Servs. Inc.</i> , 171 Wn.2d 260 (2011)	15
<i>Senate of Cal. v. Mosbacher</i> , 968 F.2d 974 (9th Cir. 1992)	8
<i>Shamrock Foods Co. v. Gast</i> , 535 F. Supp. 2d 962 (D. Ariz. 2008)	12
<i>Shell Offshore, Inc. v. Greenpeace, Inc.</i> , 709 F.3d 1281 (9th Cir. 2013)	8
<i>Stormans, Inc. v. Selecky</i> , 586 F.3d 1109 (9th Cir. 2009)	23
<i>Ticketmaster L.L.C. v. Prestige Entm’t, Inc.</i> , ___ F. Supp. 3d ___, No. 2:17-CV-07232 ODW, 2018 WL 654410 (C.D. Cal. Jan. 31, 2018).....	13
<i>Ticketmaster L.L.C. v. RMG Techs., Inc.</i> , 507 F. Supp. 2d 1096 (C.D. Cal. 2007)	9, 17, 18
<i>Triad Sys. Corp. v. Se. Express Co.</i> , 64 F.3d 1330 (9th Cir. 1995)	22
<i>United States v. Devers</i> , No. 12-CR-50-JHP, 2012 WL 12540235 (N.D. Okla. Dec. 28, 2012).....	15
<i>United States v. Nosal</i> , 676 F.3d 854 (9th Cir. 2012)	12
<i>Valle del Sol Inc. v. Whiting</i> , 732 F.3d 1006 (9th Cir. 2013)	21
<i>Van Tassell v. United Mktg. Grp., LLC</i> , 795 F. Supp. 2d 770 (N.D. Ill. 2011)	8

TABLE OF AUTHORITIES
(continued)

<i>Veridian Credit Union v. Eddie Bauer, LLC</i> , 295 F. Supp. 3d 1140 (W.D. Wash. 2017).....	15
<i>Winter v. Nat. Res. Def. Council, Inc.</i> , 555 U.S. 7 (2008).....	passim

STATUTES

15 U.S.C. § 45(n)	14
18 U.S.C. § 1030(e)(11).....	13
18 U.S.C. §§ 1030(g)	12
Computer Fraud and Abuse Act	1, 12, 13
Consumer Protection Act.....	15
Digital Millennium Copyright Act.....	17
RCW 19.86.010(2).....	15
Stored Communications Act.....	15
Washington Consumer Protection Act.....	1
Washington Unfair Competition Law.....	14

OTHER AUTHORITIES

Black’s Law Dictionary (10th ed. 2014).....	11
Federal Rule of Civil Procedure 65	2, 25

I. INTRODUCTION

At issue in this case is the right of organizations who provide information online to define and enforce the terms and conditions by which that information can be accessed and used. Plaintiff Domain Name Commission Limited (“DNCL”) is a non-profit organization based in New Zealand. Its responsibilities include regulating the use of the .nz WHOIS service, which responds to user queries by providing information about the registrants who license and use .nz domain names. DNCL fulfills this responsibility by promulgating and enforcing the .nz WHOIS Terms of Use (“TOU”), which are designed to control the dissemination of personal information and protect the privacy of .nz registrants by ensuring that only current .nz WHOIS information can be accessed and by preventing registrant details from being harvested in bulk.

Defendant DomainTools, LLC (“DomainTools”) engages in conduct that violates the TOU so that it can sell .nz registrants’ personal information. The TOU prohibit “send[ing] high volume WHOIS queries with the effect of downloading part or all of the .nz Register or collecting register data or records” and “[s]toring or compil[ing] WHOIS data to build up a secondary register of information.” Decl. of Brent Carey in Supp. of Mot. for Prelim. Inj. (“Carey Decl.”) at Ex. 5. Yet DomainTools has compiled a database that, by its own admission, is “unparalleled” in size and coverage—and thus could only have been created using high volume queries. Decl. of Todd M. Hinnen in Supp. of Mot. for Prelim. Inj. (“Hinnen Decl.”) at Ex. 1. The TOU also prohibit “publish[ing] historical or non-current versions of WHOIS data” and “publish[ing] any WHOIS data in bulk.” Carey Decl. at Ex. 5. Yet DomainTools offers a “Whois History” service allowing customers to access historical WHOIS records and a “Reverse Whois” service allowing customers to search bulk records by keyword (i.e., by registrant name).

This conduct not only constitutes a willful, ongoing breach of the TOU, it also violates the Computer Fraud and Abuse Act and the Washington Consumer Protection Act.

DomainTools’s publication in bulk and sale of .nz registrants’ personal information is irreparably harming DNCL’s reputation and goodwill by preventing DNCL from enforcing its

1 TOU, honoring its promises to .nz registrants, and protecting the privacy and safety of .nz
 2 registrants. It is also diverting DNCL's limited resources away from its organizational mission.
 3

4 Finally, the balance of equities, as well as the public interest, weigh heavily in favor of
 5 preliminary injunctive relief. DomainTools and its customers face the prospect of only minor
 6 loss of profit and inconvenience if relief is granted. Conversely, if relief is not granted, DNCL
 7 will be unable to offer its services in accordance with the TOU, unable to implement policies
 8 supported by the people and businesses of New Zealand and other .nz registrants, and unable to
 9 honor individual registrants' choice to limit access to their personal information.
 10

11 DNCL therefore moves this Court, pursuant to Federal Rule of Civil Procedure 65, for an
 12 order preliminarily enjoining DomainTools from obtaining and using .nz WHOIS records in
 13 violation of the TOU. Specifically, DNCL asks that DomainTools be enjoined from (1) accessing
 14 the .nz Register *at all* so long as its limited license remains revoked; or, in the alternative,
 15 sending automated, high-volume WHOIS queries and accessing the .nz Register in bulk in
 16 violation of the TOU; (2) storing or compiling .nz WHOIS data in its own database;
 17 (3) publishing information that has been withheld pursuant to the Individual Registrant Privacy
 18 Option ("IRPO"); (4) publishing historical versions of .nz WHOIS data through its various
 19 services; and (5) publishing .nz WHOIS data in bulk through its various services.
 20
 21
 22
 23
 24
 25
 26
 27
 28
 29
 30
 31
 32
 33
 34

35 II. STATEMENT OF FACTS

36 A. Domain Name Background and Terminology

37 This case involves technical and administrative aspects of the Internet and website
 38 registration. As such, this motion begins with a brief overview in the relevant terminology, using
 39 DNCL's own website as an illustrative example.
 40
 41
 42
 43
 44

45 To access DNCL's website, an Internet user would open a web browser and type
 46 "http://www.dnc.org.nz" into the navigation bar. This quoted series of characters is called a
 47 uniform resource locator, or URL. It is made up of several component parts that are relevant to
 48 understanding the present dispute. Carey Decl. ¶ 8.
 49
 50
 51

1 First, the URL contains a “domain name,” which is an easy-to-remember string of
2 characters that serves as a convenient alternative to a numerical IP address (the string of numbers
3 a server uses to route traffic on the Internet). In the URL “http://www.dnc.org.nz,” the domain
4 name is “dnc.org.nz.” An Internet user who continues to browse on DNCL’s website will be
5 directed to different URLs—for example, “http://www.dnc.org.nz/irpo”—but the domain name
6 for this new URL is still “dnc.org.nz.” Domain names can also be found in email addresses. *Id.*
7
8
9
10
11

12 Second, the domain name itself is split up into multiple pieces. Each piece is separated by
13 a period and is part of a hierarchical structure of domain name identifiers. The “top level”
14 domain (“TLD”) appears after the rightmost period; here, the “.nz” piece. Moreover, “.nz” is a
15 particular *type* of TLD, known as a country code top-level domain (or “ccTLD”), because it
16 indicates the country (here, New Zealand) that administers and sets policies regarding domain
17 name registration for a given website. Next comes “.org,” which is called a second-level domain.
18 Second-level domains indicate the core purpose of a website. For example, a “.org.nz” website
19 serves an organizational purpose. Finally, the “dnc” piece is called the domain “identifier,” and
20 is chosen by the individual or organization that registers and uses the domain name. *Id.* ¶ 9.
21
22
23
24
25
26
27
28
29
30

31 A nonprofit organization called the Internet Corporation for Assigned Names and
32 Numbers (“ICANN”) coordinates and maintains the Internet’s domains, including domain
33 names, ccTLDs, and TLDs. ICANN primarily operates by accrediting and imposing contractual
34 obligations on organizations known as domain “registries” and “registrars.” A domain registry
35 manages TLDs and their infrastructure by developing policy frameworks, creating domain name
36 extensions, and keeping the definitive register of domain names. A registrar issues licenses for
37 domains on behalf of domain registries to the individuals or organizations who want to use them.
38 Those individuals or organizations, in turn, are called “registrants.” Hinnen Decl. at Ex. 12.
39
40
41
42
43
44
45
46

47 Registrars and registries are required by their contracts with ICANN to operate a service
48 called WHOIS. This service allows users to search for a domain name to determine whether it is
49 currently in use and, if so, to obtain basic information about the individual or organization that
50
51

1 registered it. Specifically, it allows public access to “WHOIS information,” which typically
 2 includes (1) information about the domain name (e.g., whether it is available or in use, the date it
 3 was registered or last modified, its status, and its expiration); (2) information about the registrar
 4 (e.g., its name and contact information); and (3) information about the registrant (e.g., the name
 5 and contact information of the organization or individual currently using the domain name). *Id.*
 6
 7
 8
 9

10 **B. DNCL and the .nz WHOIS terms of use**

11 DNCL is a nonprofit entity based in New Zealand. It was created and appointed by the
 12 local ICANN-recognized registry, InternetNZ, as the sole authority for administration and
 13 management of .nz domain names on behalf of the people and businesses of New Zealand and
 14 other .nz registrants. DNCL’s organizational mission is to develop, monitor, and oversee a
 15 competitive registrar market and to create a fair environment for the registration and
 16 management of .nz domain names. Its functions include authorizing registrars to sell .nz domain
 17 name licenses to the public, outlining the policies and conditions by which persons may register
 18 domain names, and regulating the use of the .nz domain name space. Carey Decl. ¶¶ 3-7.
 19
 20
 21
 22
 23
 24
 25
 26
 27
 28

29 The public can extract WHOIS data from the .nz register via three avenues: (1) the
 30 DNCL website; (2) the .nz Port 43 service; and (3) registrars who have special access to the
 31 Query Service via SRS xml or EPP xml lookups (these are authenticated requests made against
 32 registry systems which only authorized .nz registrars can use). Importantly, although nz WHOIS
 33 information is available through other sources like registrars or third-parties like DomainTools,
 34 those sources must ultimately use one of these three avenues. *Id.* ¶ 16.
 35
 36
 37
 38
 39
 40

41 When the results of a Query Service search are provided through DNCL’s website or
 42 Port 43, the TOU are consistently displayed and inform users that they are authorized to use the
 43 .nz WHOIS service only if they comply with the requirements of the TOU. *Id.* ¶¶ 21-23.
 44
 45
 46

47 The TOU have always broadly prohibited users from “[u]sing multiple WHOIS queries,
 48 or using the output of multiple WHOIS queries in conjunction with any other facility or service,
 49
 50
 51

1 to enable or effect a download of part or all of the .nz Register.” *Id.* at Ex. 6. But the TOU were
 2 amended on June 26, 2016 to further clarify that users are prohibited from:
 3

4 Send[ing] high volume WHOIS queries with the effect of
 5 downloading part of or all of the .nz Register or collecting
 6 register data or records;
 7

8 Access[ing] the .nz Register in bulk through the WHOIS service
 9 (ie. where a user is able to access WHOIS data other than by
 10 sending individual queries to the database); . . .
 11

12 . . .
 13

14 Stor[ing] or compil[ing] WHOIS data to build up a secondary
 15 register of information;
 16

17 Publish[ing] historical or non-current versions of WHOIS data;
 18 and
 19

20 Publish[ing] any WHOIS data in bulk.
 21

22 *Id.* at Ex. 5.
 23

24 Over time, registrants in New Zealand and around the world have become increasingly
 25 concerned about publication of their personal information—especially their personal contact
 26 information—through WHOIS services. DNCL has responded to these concerns with a two-
 27 pronged approach. First, on November 28, 2017, based on extensive public input and support,
 28 DNCL launched the IRPO, which was required to be implemented by all authorized .nz registrars
 29 on March 28, 2018. The IRPO offers privacy protection for individual registrants who do not
 30 conduct “significant trade” using their.nz domain names by allowing them to withhold their
 31 detailed personal information, specifically their phone number and address, from publicly
 32 available .nz WHOIS records. The IRPO is optional, but over 11,000 domain names have been
 33 enrolled so far (about 2% of *all* registrations—including ineligible ones), and DNCL expects that
 34 number to increase significantly as the option becomes more widely known. *Id.* ¶¶ 24-41, 53, 54.
 35
 36
 37
 38
 39
 40
 41
 42
 43
 44
 45

46 Second, ever since mid-April of this year, detailed information about .nz registrants is no
 47 longer offered through Port 43. This avenue now provides only limited information about the
 48 domain itself—for example, whether the domain has been licensed or is available for use. This
 49
 50
 51

1 drastic remedy is aimed to increase DNCL's control over access and use of .nz WHOIS
 2 registrant information, and to better protect New Zealand citizens and their personal information.
 3 Even more specifically, it is meant to ensure that only current .nz WHOIS information can be
 4 accessed; and to prevent registrant details from being harvested in bulk. Notably, by combining
 5 the IRPO with strict enforcement of the TOU, DNCL empowers many .nz registrants to withhold
 6 their personal contact information altogether because the information is neither presently
 7 available nor re-creatable through historical records held by third parties. *Id.* ¶¶ 19-20.
 8
 9

10 **C. DomainTools and the present dispute.**

11 Defendant DomainTools is a Delaware limited liability company based in Seattle,
 12 Washington. DomainTools compiles and stores bulk WHOIS information from registries around
 13 the world and sells that information to individual and enterprise customers through its various
 14 research tools. Among these tools are Whois History, which allows customers to access
 15 historical WHOIS records stored in a DomainTools database; Domain Reports, which allows
 16 customers to simultaneously access all information DomainTools maintains about a particular
 17 domain—including both current and all historical WHOIS records; and Reverse Whois, which
 18 allows customers to search across WHOIS records stored in a DomainTools database and
 19 identify records matching certain keywords—including keywords that identify individual
 20 registrants. *Id.* at Exs. 2-6. DomainTools provides all of these services with respect to .nz domain
 21 names. In addition, DomainTools offers a “Whois Lookup” tool, which the public can use to
 22 obtain information about a particular domain name, including the full WHOIS record. Notably,
 23 although DomainTools does not appear to make any other changes to the WHOIS record
 24 obtained from DNCL, it strips the TOU out of the WHOIS record before displaying it in
 25 response to a search for a .nz domain. *Id.* at Exs. 7-8.
 26
 27

28 On November 2, 2017, DNCL sent a letter demanding that DomainTools cease and desist
 29 violating the TOU and infringing upon registrants' privacy or face litigation for breach of
 30 contract and violation of other laws. Although DNCL's letter set a response deadline of
 31

1 November 15, 2017, DomainTools requested several extensions, in part to discuss the possibility
 2 of resolving this matter without litigation. On April 22, 2018, well after DomainTools sent its
 3 February 7, 2018 response letter, DomainTools made clear that it would not agree to a settlement
 4 that involved complying with the TOU and applicable laws. Hinnen Decl. at Exs. 13-14.
 5
 6

7
 8 DNCL sent a final cease and desist letter on June 6, 2018, which revoked DomainTools's
 9 limited license to access the .nz WHOIS service. *Id.* at Ex. 15. When DomainTools continued to
 10 access and sell .nz WHOIS records in violation of the TOU and applicable law, DNCL filed the
 11 present lawsuit and this motion seeking preliminary injunctive relief.
 12
 13

14 III. ARGUMENT

15 A. DNCL is entitled to a preliminary injunction enjoining DomainTools's unlawful activities.

16
 17 A party seeking a preliminary injunction "must establish that he is likely to succeed on
 18 the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the
 19 balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v.*
 20 *Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008). In this case, a preliminary injunction is both
 21 necessary and appropriate because (1) DNCL is likely to succeed on the merits of its claims;
 22 (2) DNCL is currently suffering and will continue to suffer irreparable harm in the form of
 23 damage to its reputation and goodwill and frustration of its organizational mission; (3) the
 24 balance of equities tips sharply in favor of DNCL; and (4) the public interest favors issuance of
 25 an injunction pending final resolution of this action.
 26
 27

28 1. DNCL is likely to succeed on the merits of its claims.

29
 30 The first *Winter* factor—likelihood of success on the merits—is generally considered the
 31 "most important." *Garcia v. Google, Inc.*, 786 F.3d 733, 740 (9th Cir. 2015) (en banc). But a
 32 plaintiff may still obtain a preliminary injunction even when success on the merits is unlikely if
 33
 34
 35
 36
 37
 38
 39
 40
 41
 42
 43
 44
 45
 46
 47
 48
 49
 50
 51

1 there are “serious questions going to the merits,”¹ “the ‘balance of hardships tips *sharply* in the
 2 plaintiff’s favor,’ and the other two *Winter* factors are satisfied.” *See All. For the Wild Rockies v.*
 3 *Pena*, 865 F.3d 1211, 1217 (9th Cir. 2017) (quoting *Shell Offshore, Inc. v. Greenpeace, Inc.*, 709
 4 F.3d 1281, 1291 (9th Cir. 2013)).

5
 6
 7
 8
 9 As shown by even the limited evidence available without discovery, DNCL is likely to
 10 succeed on the merits of its claims or has at least raised serious questions concerning the merits.

11
 12
 13 **a. DNCL is likely to succeed on its claim that DomainTools breached**
 14 **DNCL’s terms of use.**

15
 16 A claim for breach of contract requires showing “[1] the contract imposes a duty, [2] the
 17 duty is breached, and [3] the breach proximately causes damage to the plaintiff.” *Nw. Indep.*
 18 *Forest Mfrs. v. Dep’t of Labor & Indus.*, 78 Wn. App. 707, 712 (1995).

19
 20
 21 **First**, DomainTools is bound by the duties imposed by the TOU. Whether there has been
 22 mutual assent to an online contract, including terms of use governing an online service, typically
 23 “depends on whether the user has actual or constructive knowledge of a website’s terms and
 24 conditions,” particularly where the user is not required to take affirmative action (such as a click)
 25 to agree to the terms. *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1176 (9th Cir. 2014)
 26 (quoting *Van Tassell v. United Mktg. Grp., LLC*, 795 F. Supp. 2d 770, 790 (N.D. Ill. 2011)).
 27 Courts “have consistently enforced . . . agreements where the user had actual notice of the
 28 agreement.” *Id.* And even where a user does not have actual notice, online terms of use are
 29 generally enforced “when a user is encouraged by the design and content of the website and the
 30 agreement’s webpage to examine the terms clearly available through hyperlinkage.” *McKee v.*
 31 *Audible, Inc.*, No. CV 17-1941-GW(Ex), 2017 WL 4685039, at *7 (C.D. Cal. July 17, 2017)
 32 (quoting *Berkson v. Gogo LLC*, 97 F. Supp. 3d 359, 401 (E.D.N.Y. 2015)).
 33
 34
 35
 36
 37
 38
 39
 40
 41
 42
 43
 44
 45
 46
 47
 48

49
 50
 51

 1 “Serious questions” are questions that are “substantial, difficult and doubtful, as to make them a fair
 ground for litigation and thus more deliberative investigation.” *Senate of Cal. v. Mosbacher*, 968 F.2d 974, 977-78
 (9th Cir. 1992) (internal quotation marks and citation omitted).

Here, the TOU were contained in each and every response to the voluminous number of .nz WHOIS queries that DomainTools has performed (and continues to perform), proving that DomainTools had actual notice of the terms. Indeed, DomainTools takes efforts to strip the TOU out of the “raw” .nz WHOIS records that it displays in response to queries through its “Whois Lookup” tool. *See* Hinnen Decl. ¶¶ 7-8. Under these circumstances, it would defy credulity to believe that DomainTools did not have actual notice of the TOU governing its use of the .nz WHOIS service. That the TOU did not appear until after DomainTools submitted its query is of no moment because DomainTools has been “submitting numerous queries, each of which resulted in its receiving notice of the terms [DNCL] exacted,” and because the correspondence between DNCL and DomainTools can leave no doubt that at least since November 2017 DomainTools “knew perfectly well what terms [DNCL] demanded.” *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 401 (2d Cir. 2004).

Second, even the pre-discovery evidence shows that DomainTools has violated and is continuing to violate several of the TOU’s prohibitions. Courts have recognized that entities that provide services online are entitled to set the terms of how others may permissibly use their services. *See, e.g., Register.com*, 356 F.3d at 398-401 (holding that a registrar was entitled to enforce restrictions on the use of WHOIS data as provided in its contractual terms); *Ticketmaster L.L.C. v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1113 (C.D. Cal. 2007) (holding that a plaintiff was entitled to enforce restrictions on the use of automated devices to purchase tickets from its website); *Facebook, Inc. v. Power Ventures, Inc.*, No. C 08-5780 JF (RS), 2009 WL 1299698, at *5 (N.D. Cal. May 11, 2009) (recognizing that a website was entitled to prohibit scraping activities). This case is no different: DNCL is entitled to enforce the TOU that it specifically designed to implement policies supported by members of the New Zealand online community and to protect .nz registrants’ privacy and safety.

DomainTools has been and is continuing to obtain and use .nz WHOIS data in a manner that violates at least four prohibitions in the TOU.

1 1. DomainTools violates the prohibition against “Send[ing] high volume WHOIS
2 queries with the effect of downloading part or all of the .nz Register or collecting register data or
3 records” and “Access[ing] the .nz Register in bulk through the WHOIS service.” Carey Decl. at
4 Ex. 5. The size and scope of DomainTools’s internal database establishes that DomainTools *must*
5 *have* violated these provisions. DomainTools’s website indicates that it has database records
6 pertaining to around 94% of registered .nz domains, which comports with DomainTools’s claim
7 that it has “the world’s largest database of Whois . . . records.” Hinnen Decl. at Exs. 10-11. Such
8 an “unparalleled” secondary register could only be created through the use of high volume
9 WHOIS queries. *Id.* at Ex. 1. Preliminary investigation also suggests that DomainTools takes
10 steps to evade the technical protective measures that DNCL has established to prevent high
11 volume queries and bulk harvesting of .nz WHOIS data—including by using a distributed
12 network of IP addresses from all over the world. Carey Decl. ¶ 59. Indeed, DomainTools has
13 developed means of circumventing DNCL’s technical protective measures precisely so that it can
14 submit high-volume queries and access the register in bulk in violation of the TOU.²

15 2. DomainTools violates the prohibition on “Stor[ing] or compil[ing] WHOIS data
16 to build up a secondary register of information” by creating its own database of .nz WHOIS
17 information and relying on that database to facilitate its services. *Id.* at Ex. 5. A “register” is “an
18 official list of the names of people, companies, etc.,” while a database is a “compilation of
19 information arranged in a systematic way and offering a means of finding specific elements it
20 contains, often today by electronic means.” *Register, Database*, Black’s Law Dictionary (10th
21 ed. 2014). A database that contains an official list of names and contact information is therefore
22 also a register. On its website, DomainTools states that its services rely on “records . . .
23 maintained in the DomainTools database.” Hinnen Decl. at Ex. 2. Thus, by its own admission,
24 DomainTools has compiled .nz WHOIS information in a secondary register.

25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51

² Similarly, DomainTools “[u]s[ed] multiple WHOIS queries, or us[ed] the output of multiple WHOIS queries . . . to enable or effect a download of part or all of the .nz Register,” per the earlier TOU. *Id.* at Ex. 6.

3. DomainTools violates the prohibition on “Publish[ing] historical or non-current versions of WHOIS data.” Carey Decl. at Ex. 5, by providing the Whois History tool which, in its own words, “allows DomainTools’s members access to historical Whois records” that “DomainTools has been tracking” since 1995, Hinnen Decl. at Ex 2. This unauthorized service allows any member of the public to obtain historical and non-current WHOIS data by becoming a DomainTools subscription member or ordering a Domain Report for \$49. *Id.* at Ex 5.

4. DomainTools violates the prohibition on “Publish[ing] any WHOIS data in bulk” by selling to its customers access to substantially all of the .nz WHOIS records that it has accumulated over the last twenty years and allowing them via its Reverse Whois service to search these records in bulk. Carey Decl. at Ex. 5. Neither the Whois History and Reverse Whois services would be possible if DomainTools had not submitted high-volume queries, downloaded all or a substantial portion of the register, compiled a secondary register, and published in bulk that register of non-current versions of WHOIS data to customers so that customers could run tools like Whois History and Reverse Whois against it. Carey Decl. ¶ 59.

Third, DomainTools’s conduct proximately causes ongoing and irreparable harm to DNCL. As explained in greater detail below, DomainTools is harming DNCL’s reputation and goodwill by providing services that undermine the measures .nz registrants have requested and DNCL has implemented to control dissemination of personal WHOIS information and protect the privacy of .nz registrants. DomainTools is also diverting internal resources, and thus frustrating DNCL’s organizational mission. For example, DNCL’s engineers are forced to spend time trying to detect and prevent DomainTools’s unauthorized access to and use of WHOIS services when they could otherwise spend that time serving .nz registrants and improving the DNCL website. Finally, this irreparable harm is in addition to the ongoing harm to the .nz WHOIS service that is caused by DomainTools’s repetitive queries consuming a significant portion of the capacity of the .nz WHOIS computer systems. *Id.* ¶¶ 61-73.

For these reasons, DNCL is likely to succeed on its claim that DomainTools is breaching the TOU by (1) sending automated, high-volume WHOIS queries and accessing the .nz Register in bulk; (2) storing and compiling .nz WHOIS data in its own database; (3) publishing information that has been withheld pursuant to the IRPO; (4) publishing historical versions of .nz WHOIS data; and (5) publishing .nz WHOIS data in bulk.

b. DNCL is likely to succeed on its claim that DomainTools violated the Computer Fraud and Abuse Act.

A private party may bring a claim against another private party under the Computer Fraud and Abuse Act (“CFAA”) if the plaintiff has “suffer[ed] damage or loss” from the violation aggregating to at least \$5,000 in value, and the defendant has “intentionally access[ed] a computer without authorization or exceeds authorized access and thereby obtain[ed] . . . information from any protected computer.” 18 U.S.C. §§ 1030(a)(2), 1030(g). This language “target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation.” *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (quoting *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008)).

Here, DNCL has never authorized DomainTools to access the .nz registry in the way it has—instead, DNCL has consistently forbidden DomainTools’s conduct through its TOU. In November 2017, DNCL sent a cease and desist letter notifying DomainTools that it was accessing the registry without authorization and in violation of the express terms of the TOU. When DomainTools failed to heed this warning, on June 6, 2018, DNCL revoked even its limited license to access the registry. In other words, DomainTools’s access to the registry in violation of the TOU has always been unauthorized; and now DomainTools is not authorized to access the registry at all. *See, e.g., Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016) (“[A] defendant can run afoul of the CFAA when . . . permission has been revoked explicitly.”), *cert denied*, 138 S. Ct. 313 (2017); *see also Ticketmaster L.L.C. v. Prestige Entm’t, Inc.*, __ F. Supp. 3d __, No. 2:17-CV-07232 ODW (JCx), 2018 WL 654410, at *6 (C.D. Cal. Jan. 31, 2018) (dismissing plaintiff’s CFAA claims because plaintiff “ha[d] not shown that it

1 rescinded permission from Defendants to use its website” so its claims were based entirely on the
 2 TOU). Yet DomainTools continues to access the registry without authorization—even going so
 3 far as to employ technical measures to evade IP-blocking (and IP-rate limiting). *Compare*
 4 *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 969-70 (N.D. Cal. 2013) (finding
 5 unauthorized access where defendants ignored cease and desist letters and evaded technological-
 6 blocking measures), *with hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1113 (N.D.
 7 Cal. 2017) (justifying its conclusion that the CFAA may not be implicated on the grounds that a
 8 website could employ *effective* “anti-bot measures to prevent . . . harmful intrusions”), *appeal*
 9 *docketed*, No. 17-16783 (9th Cir. Sept. 6, 2017).

10 DomainTools’s unlawful conduct has caused DNCL to suffer losses exceeding \$5,000
 11 over a one-year period. *See* 18 U.S.C. § 1030(e)(11) (defining “loss” to mean “any reasonable
 12 cost to any victim, including the cost of responding to an offense, conducting a damage
 13 assessment, and restoring the data, program, system, or information to its condition prior to the
 14 offense, and any revenue lost, cost incurred, or other consequential damages incurred because of
 15 interruption of service”). DNCL estimates that its employees have spent in excess of 320 hours
 16 analyzing, investigating, and responding to DomainTools’s actions over the past year. *Cf. e.g.*,
 17 *Facebook*, 844 F.3d at 1066 (finding plaintiff suffered “loss” due to the “many hours” employees
 18 spent “analyzing, investigating, and responding to [defendant]’s actions,” even where there was
 19 no interruption in service). Because DNCL employees are paid, on average, around \$139 USD
 20 per hour, this cost alone easily surpasses the statutory threshold—amounting to over \$44,500.
 21 Carey Decl. ¶¶ 63-73. Additionally, each query to the .nz WHOIS servers costs computing
 22 power, disrupts network transmissions, and otherwise interferes with technical infrastructure.

23
 24
 25
 26
 27
 28
 29
 30
 31
 32
 33
 34
 35
 36
 37
 38
 39
 40
 41
 42
 43
 44
 45 **c. DNCL is likely to succeed on its claim that DomainTools violated the**
 46 **Washington Unfair Competition Law.**

47 “To prevail on a CPA action, the plaintiff must prove an ‘(1) unfair or deceptive act or
 48 practice; (2) occurring in trade or commerce; (3) public interest impact; (4) injury to plaintiff in
 49
 50
 51

1 his or her business or property; [and] (5) causation.” *Klem v. Wash. Mut. Bank*, 176 Wn.2d 771,
 2 782 (2013) (citation omitted). All these elements are met here.

3
 4 **First**, harvesting the registration data of individual registrants in bulk and retaining it
 5 after the registrant has chosen to make that information private comprises an unfair act or
 6 practice. To determine whether a practice or act is “unfair,” Washington courts are “guided by
 7 federal law in the area.” *Klem*, 176 Wn.2d at 787. For example, courts have looked to the Federal
 8 Trade Commission for guidance and considered:
 9

10 (1) whether the practice, without necessarily having been previously
 11 considered unlawful, offends public policy as it has been established
 12 by statutes, the common law, or otherwise—whether, in other
 13 words, it is within at least the penumbra of some common-law,
 14 statutory, or other established concept of unfairness; (2) whether it
 15 is immoral, unethical, oppressive, or unscrupulous; (3) whether it
 16 causes substantial injury to consumers (or competitors or other
 17 businessmen).

18 *Magney v. Lincoln Mut. Sav. Bank*, 34 Wn. App. 45, 57 (1983) (quoting *Fed. Trade Comm’n v.*
 19 *Sperry & Hutchinson Co.*, 405 U.S. 233, 244 n.5 (1972)); *see also Klem*, 176 Wn.2d at 787
 20 (“Current federal law suggests a ‘practice is unfair [if it] causes or is likely to cause substantial
 21 injury to consumers which is not reasonably avoidable by consumers themselves and not
 22 outweighed by countervailing benefits.’” (quoting 15 U.S.C. § 45(n))). DomainTools’s practices
 23 are likely to cause substantial injury to consumers—including approximately 715 Washington
 24 consumers—by infringing their privacy rights and making publicly available information that
 25 those consumers have chosen to withhold through the IRPO setting. *See Carey Decl.* ¶ 88; *cf.*
 26 *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 668 (D.N.J. 2013)
 27 (“Facebook wall posts that are configured to be private are, by definition, not accessible to the
 28 general public [and thus covered by the Stored Communications Act]. . . [because] the
 29 communicator took steps to keep [them] private.”); *United States v. Devers*, No. 12-CR-50-JHP,
 30 2012 WL 12540235, at *2 (N.D. Okla. Dec. 28, 2012) (acknowledging that Facebook users
 31 might have a reasonable expectation of privacy if they elect the most stringent privacy setting);
 32
 33
 34
 35
 36
 37
 38
 39
 40
 41
 42
 43
 44
 45
 46
 47
 48
 49
 50
 51

1 *see also Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1162 (W.D. Wash.
2
3 2017) (noting “the liberal construction the court applies to the CPA”).³

4
5 **Second**, DomainTools engages in this unfair act or practice for the purpose of providing
6
7 products and services to paying customers, and thus “in trade or commerce.” *See* RCW
8
9 19.86.010(2) (“‘Trade’ and ‘commerce’ shall include the sale of assets or services, and any
10
11 commerce directly or indirectly affecting the people of the state of Washington.”); *Michael v.*
12
13 *Mosquera-Lacy*, 165 Wn.2d 595, 602-03 (2009) (“The term ‘trade’ as used by the Consumer
14
15 Protection Act includes . . . the entrepreneurial or commercial aspects of professional services.”
16
17 (quoting *Ramos v. Arnold*, 141 Wn. App. 11, 20 (2007))).

18
19 **Third**, the nature of this action means that “the public was integrally involved because of
20
21 this essentially private dispute.” *Nordstrom, Inc. v. Tampourlos*, 107 Wn.2d 735, 742-43 (1987)
22
23 (holding that “confusion of the public, absent some unusual or unforeseen circumstances, will be
24
25 sufficient to meet the public interest requirement of the [Washington] Consumer Protection
26
27 Act”). This action is being brought by DNCL to, among other things, vindicate the policy
28
29 developed and implemented based on the input of consumers of .nz registry services and the
30
31 privacy and safety interests of individual registrants; it thus implicates the public interest.

32
33 **Fourth and Fifth**, DomainTools’s conduct has proximately caused injury to DNCL in its
34
35 business or property. As explained above, DomainTools is preventing DNCL from providing its
36
37 services in accordance with the TOU and IRPO implemented in response to privacy and safety
38
39 concerns raised by the people and businesses of New Zealand and other .nz registrants.
40
41 DomainTools is also diverting employee time, disrupting network transmissions and damaging
42
43 the .nz WHOIS technical infrastructure. Finally, as explained further below, DomainTools’s
44

45
46 ³ Even if Washington consumers were not directly affected, Washington courts have recognized that a non-
47
48 resident can bring a CPA claim in cases like this where “Washington State has a strong interest in enforcing its laws
49
50 against its [own] businesses, lest the state ‘become a harbor for businesses engaging in unscrupulous practices out of
51
state.”” *Rajagopalan v. NoteWorld, LLC*, No. C11-05574BHS, 2012 WL 727075, at *5 (W.D. Wash. Mar. 6, 2012),
aff’d, 718 F.3d 844 (9th Cir. 2013) (quoting *Schnall v. AT&T Wireless Servs. Inc.*, 171 Wn.2d 260, 287 (2011)
(Sanders, J., dissenting)).

activities are causing reputational harm and loss of goodwill to DNCL. *See Nordstrom*, 107 Wn.2d at 740 (noting that “loss of goodwill suffice[s]” to show injury to business or property).

2. DNCL is currently suffering and will continue to suffer irreparable harm without a preliminary injunction.

The second *Winter* factor requires a plaintiff to “demonstrate immediate threatened injury as a prerequisite to preliminary injunctive relief.” *Caribbean Marine Servs. Co. v. Baldrige*, 844 F.2d 668, 674 (9th Cir. 1988). “[E]conomic injury alone does not support a finding of irreparable harm, because such injury can be remedied by a damage award.” *Rent-A-Ctr., Inc. v. Canyon Television & Appliance Rental, Inc.*, 944 F.2d 597, 603 (9th Cir. 1991).

DNCL is currently suffering and will continue to suffer irreparable harm absent a preliminary injunction. Specifically, DomainTools is harming DNCL’s reputation and goodwill in the New Zealand online community by disseminating the WHOIS information of .nz registrants who elected to keep that information private, and by generally offering services in violation of the TOU. Moreover, as discussed below, DomainTools is also undermining publicly supported DNCL policies and diverting internal resources, thus frustrating DNCL’s organizational mission. None of these harms can be remedied by a damage award; they can only be remedied by preliminary and, ultimately, permanent injunctive relief.

a. DomainTools is causing irreparable harm to DNCL’s reputation and goodwill by depriving IRPO registrants of the privacy protection DNCL promised them.

First, if DomainTools is permitted to continue its activities, DNCL will continue to face irreparable harm to its reputation and goodwill because it will be unable to implement the policy supported by .nz users and unable to deliver on the promises it made to IRPO registrants.

The Ninth Circuit has consistently recognized that “loss of control over business reputation and damage to goodwill can constitute irreparable harm.” *adidas Am., Inc. v. Skechers USA, Inc.*, 890 F.3d 747, 756 (9th Cir. 2018) (alterations omitted) (quoting *Herb Reed Enters., LLC v. Fla. Entm’t Mgmt., Inc.*, 736 F.3d 1239, 1250 (9th Cir. 2013)). It has also specifically

1 recognized that a third party can damage an entity's reputation and goodwill by wrongfully
 2 interfering with its contractual obligations.
 3

4 For example, in *Disney Enterprises, Inc. v. VidAngel, Inc.*, 869 F.3d 848 (9th Cir. 2017),
 5 the defendant operated an unauthorized online streaming service that censored movies and
 6 television shows. Disney and other plaintiffs sued under the Digital Millennium Copyright Act.
 7 The district court granted a preliminary injunction, and the Ninth Circuit affirmed, on the ground
 8 that "VidAngel's service undermine[d the Studios'] negotiating position . . . and also damage[d]
 9 goodwill with licensees, because it offer[ed] the Studios' works during negotiated 'exclusivity
 10 periods.'" *Id.* at 865 (internal quotation marks omitted). In other words, VidAngel irreparably
 11 harmed Disney's reputation by making it impossible for Disney to deliver on its promises.
 12

13 A similar rationale was approved in *Ticketmaster L.L.C. v. RMG Techs., Inc.*, 507 F.
 14 Supp. 2d 1096 (C.D. Cal. 2007), where Ticketmaster alleged that its competitor, RMG,
 15 developed and used automated devices to access Ticketmaster's website and purchase tickets en
 16 masse. As here, this activity violated the website's terms of use and several state and federal
 17 laws, *see id.* at 1102, and, as in *Disney*, the district court found irreparable harm to reputation due
 18 to interference with contractual promises. Specifically, Ticketmaster's terms of use assured
 19 customers that they were all on a level playing field, and that tickets could not be purchased en
 20 masse by sophisticated entities. But RMG's activities in violation of the terms of use made it
 21 impossible for Ticketmaster to deliver on these promises. Ticketmaster showed "that it [was]
 22 suffering a loss of goodwill with the buying public [due to] a growing public perception that
 23 [Ticketmaster did] not provide the public with a fair opportunity to buy tickets due to automated
 24 purchases." *Id.* at 1114. The court relied on this showing of harm to preliminarily enjoin RMG
 25 from making automated purchases in violation of Ticketmaster's terms of use.
 26

27 The situation is the same in this case. Over the past few years, Internet users in New
 28 Zealand have voiced intense concern about dissemination of WHOIS information—specifically
 29 citing privacy and safety concerns—and have demanded a change to .nz policies. *See Carey*
 30
 31

Decl. Ex. 23. DNCL responded by implementing the IRPO, which assures eligible registrants that their detailed contact information will be not be accessible absent a specific, justified request for that information. Yet registrants are not receiving that benefit. Instead, they are subjected to continued publication of their detailed contact information, which was collected by DomainTools en masse and compiled in violation of the TOU. And to make matters worse, rather than apologizing for its wrongful profiteering, DomainTools continues to boast about how it has unraveled the “cloak[] [of] privacy” offered by the IRPO. Hinnen Decl. at Ex. 9. In sum, like VidAngel and RMG, DomainTools is harming DNCL’s reputation and goodwill by selling services that undermine the promises made to IRPO registrants.

b. DomainTools is causing DNCL to suffer irreparable harm to its reputation and goodwill because .nz registrants are not receiving the general protections promised in the TOU.

In addition to undermining DNCL’s ability to deliver on the specific promises made to IRPO registrants, DomainTools is undermining DNCL’s ability to deliver on the general promises made to all registrants through the TOU.

DNCL has implicitly promised all .nz registrants (1) that only current WHOIS information will be made publicly available, and (2) that WHOIS information can only be accessed via specific, individualized queries; not via mass, systematic queries. These terms are material to registrants’ decisions regarding whether to register their domain with .nz or with another registry.

Registrants are more likely to register a .nz website because (1) they are promised that WHOIS information will no longer be available once a domain becomes inactive, and (2) they are promised that sophisticated entities cannot collect WHOIS information en masse and compile it for commercial use. Conversely, if these assurances do not exist, then registrants are more likely to use another registry, such as “.com,” which allows registrants to use a proxy service. (A proxy service allows registrants to use the contact information of a designated entity instead of their own.) These services are not allowed with respect to .nz domains, in part because DNCL

believes registrants are sufficiently protected by its TOU. As shown through public comments, if DomainTools continues to subvert DNCL's TOU, registrants may prefer to use other registers. See Carey Decl. ¶ 76(a) ("Had I known this, I would NOT have bought [a .nz] domain name."); *id.* ¶ 76(d) ("I have a .com website and they manage to keep our details private . . .").

The TOU are thus material to .nz registrants. And because they are material, DNCL faces irreparable harm to its reputation and goodwill if DomainTools is allowed to continually undermine them and offer services based on information registrants have chosen to withhold.

The Second Circuit has affirmed preliminary injunctive relief in a remarkably similar situation. See *Register.com, Inc.*, 356 F.3d 393. Like DNCL, Register.com offered free WHOIS services. And like DNCL, its terms of use specifically prohibited "high volume, automated, electronic processes," and "[t]he compilation, repackaging, dissemination or other use of [WHOIS information]." *Id.* at 420 (Parker, J., draft opinion). Register.com filed suit against Verio for violating these provisions, and the trial court granted a preliminary injunction. *Id.* at 396. The Second Circuit affirmed, agreeing that Verio was bound by the terms of use and that Register.com would face irreparable harm if Verio were permitted to continue ignoring the above restrictions. The court cited both immediate, direct harm via "the loss of Register.com's relationships with customers and co-brand partners" due to Verio's violation of the various terms of use, and the possibility of future harm to server capacity if other service providers followed Verio's lead and submitted mass queries in violation of the terms of use. See *id.* at 404.

DNCL faces immediate and direct harm to its reputation and goodwill for similar reasons here. Moreover, DNCL faces the prospect of exacerbated harm in the future. If DomainTools continues its unauthorized access and use, then other Internet service providers may follow suit, and registrants will (correctly) conclude that DNCL has completely lost the ability to control access and use of the WHOIS information on its website.

The Ninth Circuit has affirmed preliminary injunctions based on much less severe reputational harm than this. For example, in *Regents of University of California v. American*

1 *Broadcast Companies, Inc.*, 747 F.2d 511, 520 (9th Cir. 1984), it affirmed a trial court’s
 2 determination that the University of Nebraska and the University of Notre Dame could cause
 3 irreparable harm to the University of Southern California (“USC”) by refusing to allow
 4 basketball games between these schools to be broadcast. The Ninth Circuit accepted that this
 5 refusal could lead to severe reputational harm even though it only applied to basketball—as
 6 opposed to other athletic programs; and even though it only applied to two universities—as
 7 opposed to all of USC’s competitors. *See id.* at 520. If a well-rounded institution like USC could
 8 suffer a “palpable diminution in [its] national reputation” due to such a minor slight, then it goes
 9 without saying that a single-mission entity like DNCL will suffer irreparable reputational harm if
 10 DomainTools is permitted to undermine the TOU designed to protect .nz registrants.

21 **c. DomainTools is causing DNCL irreparable harm because it will be**
 22 **forced to divert internal resources away from its organizational**
 23 **mission to police and prevent DomainTools’s unauthorized activity.**

24 In addition to affirming preliminary injunctive relief based on reputational harm, the
 25 Ninth Circuit has also affirmed relief on the ground that a nonprofit organization is irreparably
 26 harmed when its “ability to carry out [its] mission[]” is “impaired.” *See Valle del Sol Inc. v.*
 27 *Whiting*, 732 F.3d 1006, 1018 (9th Cir. 2013).

28 In *Valle del Sol*, a church, its pastor, and its staff members sued the State of Arizona,
 29 arguing that a state statute—which prohibited illegally concealing, harboring, shielding, or
 30 transporting an alien in Arizona in furtherance of the alien’s unlawful presence in the United
 31 States—was unconstitutionally vague. The trial court and the Ninth Circuit agreed that the
 32 plaintiffs were likely to succeed on the merits of this claim and would suffer irreparable harm
 33 absent an injunction. Among other things, the church would lose volunteers who feared
 34 prosecution under the statute and be “required to divert resources to educate its members [about
 35 the statute] and counteract this frustration of its mission.” *Id.* at 1018.

36 Similarly here, DNCL has been “perceptibly impaired” in its “ability to carry out [its]
 37 mission[],” *id.*, because it has been forced to allocate organizational time and leadership to try to

1 stay one step ahead of DomainTools. Specifically, DNCL has been forced to modify the Port 43
 2 command line query, refine its rate-limiting measures, send demand letters, and travel to Seattle
 3 to meet with DomainTools. Carey Decl. ¶¶ 19, 71, 93-94. All this time and energy would be
 4 better spent carrying out DNCL's organizational mission—which is to administer and manage
 5 .nz domain names and serve New Zealand Internet users. Once again, DNCL faces the prospect
 6 of continuing irreparable harm absent a preliminary injunction.
 7
 8
 9
 10
 11
 12

13 **3. The balance of equities tips sharply towards DNCL.**

14 The third *Winter* factor requires this court to “balance the interests of all parties and
 15 weigh the damage to each.” *See L.A. Mem'l Coliseum Comm'n v. Nat'l Football League*, 634
 16 F.2d 1197, 1203 (9th Cir. 1980). Ordinarily, the party seeking an injunction need only show the
 17 injunction would “do more good than harm.” *All. for the Wild Rockies v. Cottrell*, 632 F.3d 1127,
 18 1133 (9th Cir. 2011). But where a party has only shown serious questions concerning the merits
 19 of a claim, under the sliding scale variant of the *Winter* standard, the party must show the
 20 “balance of hardships tips sharply in [its] favor.” *Pena*, 865 F.3d at 1217 (emphasis omitted).
 21
 22
 23
 24
 25
 26
 27
 28

29 DNCL meets either standard. As demonstrated above, DNCL faces continuing irreparable
 30 harm to its reputation, goodwill, and organizational mission because .nz individual registrants are
 31 being deprived of the data protection that they requested and have been promised. The severity
 32 of this harm has been made clear above.
 33
 34
 35
 36

37 Conversely, DomainTools will suffer either no harm or very limited pecuniary harm.
 38 DNCL has only asked this Court to enjoin DomainTools from violating the TOU by offering the
 39 offending services for .nz domains.⁴ If DNCL succeeds in its claims, DomainTools is not harmed
 40 because it had no right to offer these services in the first place. *See Triad Sys. Corp. v. Se.*
 41
 42
 43
 44
 45
 46
 47
 48

49 ⁴ In its complaint, DNCL also demands that DomainTools delete all historical .nz WHOIS records obtained
 50 and stored in violation of the .nz WHOIS TOU. But for now, a cessation of continuing activities will prevent further
 51 harm pending a final judgment. *See Perfect 10, Inc. v. Google, Inc.*, 653 F.3d 976, 981-82 (9th Cir. 2011).

1 *Express Co.*, 64 F.3d 1330, 1338 (9th Cir. 1995) (“[L]ost profits from an activity which has been
2 shown likely to be [unlawful] . . . merit[] little equitable consideration.”).

3
4 But even if DomainTools ultimately prevails, it would suffer very limited harm.
5
6 Specifically, it would suffer only the loss of profits that it would have otherwise earned by
7 offering the offending services with respect to .nz domains. To put the effect in perspective—
8
9 DomainTools maintains more than 200 times as many records about *commercial* domain names
10 hosted on a United States register as about *any* domain names hosted on the New Zealand
11 register. Hinnen Decl. at Ex. 11. The effect of an injunction on DomainTools’s global domain
12 services would therefore be largely imperceptible. And more significantly, unlike the harm
13 suffered by DNCL, such harm could be easily remedied after the fact through a monetary award.
14
15

16 The balance of equities thus tips—sharply or otherwise—in DNCL’s favor.
17
18

19
20
21 **4. A preliminary injunction is in the public interest.**
22

23 The final *Winter* factor instructs that, if preliminary relief would “reach[] beyond the
24 parties, carrying with it a potential for public consequences,” *Boardman v. Pac. Seafood Grp.*,
25 822 F.3d 1011, 1023–24 (9th Cir. 2016) (quoting *Stormans, Inc. v. Selecky*, 586 F.3d 1109, 1139
26 (9th Cir. 2009)), then the court must consider whether preliminary relief is in the public interest.
27 Here, preliminary relief would both reach beyond the parties and be in the public interest.
28
29

30 Most obviously, preliminary relief would affect non-party .nz registrants and
31 DomainTools customers. The interests of these third parties largely mirror those of the parties.
32 On the one hand, if a preliminary injunction is not granted, .nz registrants face continued
33 unauthorized access and use of their personal WHOIS information. Surveys conducted for the
34 New Zealand Office of Privacy Commissioner have confirmed that many New Zealand residents
35 (who are the majority of .nz registrants) are concerned about unfettered online dissemination of
36 their personal information—especially their contact information. Carey Decl. at Ex. 23.
37
38

39 On the other hand, if a preliminary injunction is granted, DomainTools’s customers will
40 be unable to purchase the offending services with respect to .nz domains. As discussed above,
41
42
43
44
45
46
47
48
49
50
51

1 this outcome will not adversely affect their interests at all if DNCL succeeds in the underlying
2 litigation—as is likely. Moreover, even in the unlikely event that DNCL fails, a wrongful
3 injunction would amount to little more than an apparent inconvenience for DomainTools’s
4 customers. Such customers could still obtain current .nz WHOIS information (minus information
5 withheld pursuant to the IRPO) through DNCL’s website and, when appropriate, historical and
6 withheld .nz WHOIS information by making a request to DNCL. *Id.* ¶¶ 42-51. The information
7 regarding .nz registrants available through DNCL is more current and accurate than that
8 available through DomainTools, which continues to publish historical (and therefore potentially
9 outdated) information. DomainTools’s customers, including law enforcement and other public
10 interest organizations, will receive more accurate information (for free and without violating the
11 TOU) through DNCL, which will lead to more fruitful investigations and fewer spurious claims
12 based on outdated and inaccurate information against current and former .nz registrants.
13

14 But preliminary relief would reach even further beyond the parties: The decision to grant
15 or deny a preliminary injunction affects the global Internet community.
16

17 This action has been brought at a pivotal moment in public discourse. The world has
18 changed drastically over the last twenty years since WHOIS information first became available,
19 and the public has grown increasingly concerned about unfettered access to private personal
20 information online. The European Union passed the European General Data Protection
21 Regulation (“GDPR”) to address these very concerns—broadly prohibiting companies from
22 publishing online identifying information collected from EU citizens in EU member states absent
23 prior express consent. Many registries have in turn responded to the GDPR by revising their
24 terms of use to limit access to personal WHOIS information. Hinnen Decl. ¶ 12, Ex. 11.
25

26 Similarly, although ICANN has historically required all accredited registries and
27 registrars to make WHOIS information publicly available, it has responded to the shift in public
28 opinion by taking steps to increase control over the public disclosure of WHOIS information.
29 Specifically, ICANN has adopted an interim “tiered access” model, which would restrict access
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51

1 to detailed WHOIS information to those approved through a special accreditation process. *Id.* In
 2 other words, ICANN hopes to essentially press the “reset” button on the public availability of
 3 personal WHOIS information and implement a regime very like that currently offered by DNCL.
 4

5 DomainTools’s offending services could vitiate these efforts. If courts are not willing to
 6 bind DomainTools to the TOU to which it agreed, then DomainTools can simply rely on its
 7 secondary registry to recreate and publicize records that ICANN and other Internet actors are
 8 working to protect. Ironically, DomainTools would reap the benefits of its unlawful conduct,
 9 becoming a rare or sole source of private registrant information that registrants and registries
 10 have chosen not to make publicly available. DNCL is therefore not the only organization that
 11 would benefit from a preliminary injunction here. Instead, the entire global Internet community
 12 benefits from an order holding DomainTools to its contractual obligations and honoring the
 13 choice .nz registrants have made to protect their private information.
 14

15 **B. No bond should be required.**

16 Federal Rule of Civil Procedure 65(c) requires, as a condition to issuance of a
 17 preliminary injunction, that the Court require the applicant to provide security “in an amount that
 18 the court considers proper to pay the costs and damages sustained by any party found to have
 19 been wrongfully enjoined or restrained.” Where, as here, the plaintiff is likely to prevail on the
 20 merits and there is no likelihood of harm to the defendant from issuance of a preliminary
 21 injunction, the Court has broad discretion to require no bond or other security. *Cal. ex rel. Van*
 22 *De Kamp v. Tahoe Reg’l Planning Agency*, 766 F.2d 1319, 1325-26 (9th Cir. 1985).
 23

24 As demonstrated above, DNCL is likely to succeed on its claims due to DomainTools’s
 25 continued and brazen violation of its TOU. DNCL also faces the prospect of irreparable harm to
 26 its reputation, goodwill, and nonprofit mission if preliminary relief is not granted; while if it is
 27 granted, DomainTools faces, at most, only minor loss of profits. In light of this sharply tipped
 28 balance of equities and the strong public interest in holding DomainTools to its contractual
 29 obligations to safeguard personal .nz WHOIS information, no bond should be required.
 30
 31
 32
 33
 34
 35
 36
 37
 38
 39
 40
 41
 42
 43
 44
 45
 46
 47
 48
 49
 50
 51

IV. CONCLUSION

For the foregoing reasons, DNCL respectfully requests that its motion for a preliminary injunction be granted.

RESPECTFULLY SUBMITTED this 15th day of June, 2018.

s/ Todd M. Hinnen

Todd M. Hinnen, WSBA No. 27176

Erin K. Earl, WSBA No. 49341

Anna Mouw Thompson, WSBA No. 52418

Attorneys for Plaintiff Domain Name

Commission Limited

Perkins Coie LLP

1201 Third Avenue, Suite 4900

Seattle, WA 98101-3099

Telephone: 206.359.8000

Facsimile: 206.359.9000

Email: THinnen@perkinscoie.com

EEarl@perkinscoie.com

AnnaThompson@perkinscoie.com

Attorneys for Plaintiff

Domain Name Commission Limited

CERTIFICATE OF SERVICE

I certify under penalty of perjury that on June 15, 2018, I electronically filed the foregoing PLAINTIFF DOMAIN NAME COMMISSION LIMITED'S MOTION FOR PRELIMINARY INJUNCTION and served the same by the method(s) indicated below.

Jacob Heath
Aravind Swaminathan
Orrick, Herrington & Sutcliffe, LLP
701 5th Ave
Suite 5600
Seattle, WA 98104

Attorneys for Defendant DomainTools, LLC

☒ Via hand delivery
☐ Via U.S. Mail, 1st Class, Postage Prepaid
☐ Via Overnight Delivery
☐ Via Facsimile
☐ Via Email
☐ Other: _____

DATED this 15th day of June, 2018.

s/ Todd M. Hinnen

Todd M. Hinnen, WSBA No. 27176
Attorneys for Domain Name Commission
Limited

Perkins Coie LLP

1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099

Telephone: 206.359.8000

Facsimile: 206.359.9000

E-mail: THinnen@perkinscoie.com

CERTIFICATE OF SERVICE
(NO. 2:18-CV-874) – 1

139655561.8

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000